

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-222065

(43)公開日 平成10年(1998)8月21日

(51)Int.CL⁶

G 0 9 C 1/00

識別記号

6 5 0

6 3 0

P I

G 0 9 C 1/00

6 5 0 A

6 3 0 Z

審査請求 未請求 請求項の数13 OL (全 7 頁)

(21)出願番号

特開平9-20607

(22)出願日

平成9年(1997)2月9日

(71)出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(71)出願人 591230295

エヌティティエレクトロニクス株式会社

京都府伏見区桜丘町20番1号

(72)発明者 石井 駿司

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 田中 淳人

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74)代理人 弁理士 伊東 忠彦

最終頁に続く

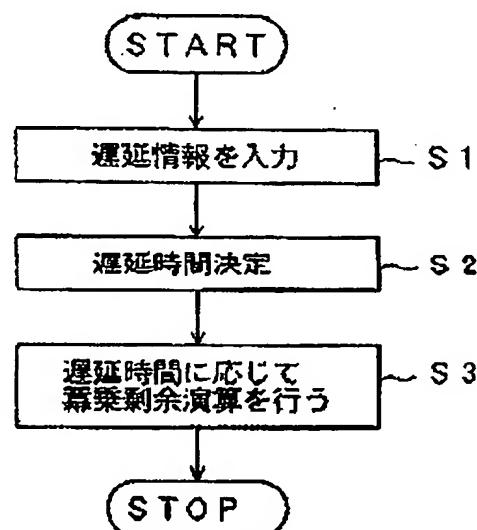
(54)【発明の名称】 幕張剰余演算方法及び装置

(57)【要約】

【課題】 専用プロセッサを利用した幕張演算を利用した公開鍵暗号の攻撃方法として、同じパラメータを利用して秘密鍵を求めるようなタイミングアタックに対する防御が可能な幕張剰余演算方法及び装置を提供する。

【解決手段】 本発明は、幕張剰余演算毎に伝播遅延によるクリティカルバスの遅延時間を変化させる。そのため、幕張剰余の演算時間を変化させるための遅延情報を入力し、入力された遅延時間に基づいて遅延時間を見定し、決定された遅延時間に応じて演算に適用する遅延時間を見せて幕張剰余演算を行う。

本発明の原理を説明するための図



【特許請求の範囲】

【請求項1】 公開鍵暗号の基本演算である幕乗剰余演算方法において、

幕乗剰余演算毎に伝送遅延によるクリティカルバスの遅延時間を変化させることを特徴とする幕乗演算方法。

【請求項2】 幕乗剰余の演算時間を変化させるための遅延情報を入力し、

入力された前記遅延時間に基づいて遅延時間を決定し、決定された遅延時間に応じて、演算に適用する遅延時間を変化させて幕乗剰余演算を行う請求項1記載の幕乗剰余演算方法。 10

【請求項3】 亂数を生成するために必要な初期値を生成し、

前記初期値に基づいて乱数を生成し、

生成した前記乱数から前記遅延時間を生成する請求項2記載の幕乗剰余演算方法。

【請求項4】 前記乱数生成に用いる前記初期値を生成する際に、

複数の初期値を生成し、

生成された前記複数の初期値から乱数を生成する請求項1、2及び3記載の幕乗剰余演算方法。 20

【請求項5】 前記乱数生成に用いる前記初期値を生成する際に、

前記幕乗剰余演算中に前記初期値を更新する請求項1、2、3及び4記載の幕乗剰余演算方法。

【請求項6】 前記初期値を更新する際に、

前記幕乗剰余演算中の途中結果の一部または、全部を用いて、以降の乱数の初期値を更新する請求項5記載の幕乗剰余演算方法。

【請求項7】 幕乗剰余演算を実行する幕乗剰余演算装置であって、

幕乗剰余の演算時間を変化させるための情報を入力する変化情報入力手段と、

前記変化情報入力手段により入力された前記変化情報に基づいて遅延時間を決定する遅延時間決定手段と、

前記遅延時間決定手段により決定された前記遅延時間に基づいて幕乗剰余演算を行う幕乗剰余演算手段とを有することを特徴とする幕乗剰余演算装置。 30

【請求項8】 前記変化情報入力手段は、

乱数を生成するために必要な初期値を入力する乱数初期値入力手段と、

前記乱数初期値入力手段により入力された前記初期値に基づいて乱数を生成し、前記変化情報として前記遅延時間決定手段に入力する乱数生成手段とを含み、

前記遅延時間決定手段は、

前記乱数生成手段により入力された前記乱数に基づいて遅延時間を決定する手段を含む請求項7記載の幕乗剰余演算装置。

【請求項9】 前記乱数初期値入力手段は、

乱数を生成するために必要な初期値を外部から入力する 50

第1の乱数初期値入力手段を含む請求項8記載の幕乗剰余演算装置。

【請求項10】 前記乱数初期値入力手段は、乱数を生成するための必要な初期値を装置内部で生成する第2の乱数初期値入力手段を含む請求項8記載の幕乗剰余演算装置。

【請求項11】 前記乱数初期値入力手段は、前記第1の乱数初期値入力手段により入力された前記初期値と、前記第2の乱数初期値入力手段により入力された前記初期値とを合成した値を前記乱数生成手段への入力とする初期値合成手段を含む請求項8、9及び10記載の幕乗剰余演算装置。

【請求項12】 前記遅延時間決定手段は、前記幕乗剰余演算手段の実行中に前記遅延時間を更新する遅延時間更新手段を含む請求項7記載の幕乗剰余演算装置。

【請求項13】 前記変化情報入力手段は、前記幕乗剰余演算手段の実行中の演算結果を用いて、以降の前記乱数生成手段の初期値を更新する演算結果循環型初期値更新手段を含む請求項7記載の幕乗剰余演算装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、幕乗剰余演算方法及び装置に係り、特に、RSA暗号等の公開鍵暗号の基本演算である幕乗剰余演算において、演算時間から不正に秘密鍵を推測されることを防止するための幕乗剰余演算方法及び装置に関する。

【0002】

【従来の技術】 幕乗剰余演算は、公開鍵暗号の基本演算として非常によく利用されるようになっている。RSA暗号を例にすると、復号演算及び署名演算をする場合、署名を秘密とした幕乗剰余演算を行う。

【0003】 従来、公開鍵暗号の暗号が幕乗剰余演算を利用している。幕乗剰余演算は、

$$a^b \bmod c$$

と表すことができる。署名演算あるいは、復号演算に関して少なくとも1つのパラメータは秘密である。

【0004】

【発明が解決しようとする課題】 しかしながら、3つのパラメータが全く同じ場合、当然同一の結果が得られる。また、専用プロセッサを用いて幕乗剰余演算を行う場合には、動作周波数等の環境を一定にすれば、必ず同一の演算結果が得られる。この特徴を利用して秘密鍵を求めることができるという指摘が、"Paul C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", Advances in Cryptology: Proceedings of Crypto 96, Plenum Press, 1996, p.104-113"で報告されている。この方法(タイミングアタックと呼ぶことにする)は、多少時間がかかり容易

八、六、

ではないが、数学的な特徴を利用して、秘密鍵を導出しようとしたり、秘密鍵の全数検索をしたりする方法よりは、はるかに簡単である。この方法は、より正確に時間を計測できる環境である程、危険性が増す。また、並列ジョブが少ないほど危険性が高い。

【0005】このように、乗乗剰余演算等を利用する秘密鍵演算は、全て同じパラメータを利用すれば、演算量は同じである。この特徴を悪用され、秘密鍵を求めることが出来る場合がある。本発明は、上記の点に鑑みなされたもので、専用プロセッサにおける乗乗演算を利用した公開鍵暗号の攻撃方法として、同じパラメータを利用して秘密鍵を求めるようなタイミングアタックに対する防御が可能な乗乗剰余演算方法及び装置を提供することを目的とする。

【0006】

【課題を解決するための手段】図1は、本発明の原理を説明するための図である。本発明は、公開鍵暗号の基本演算である乗乗剰余演算方法において、乗乗剰余演算毎に伝播遅延によるタリティカルパスの遅延時間を変化させる。

【0007】本発明は、乗乗剰余の演算時間を変化させるための遅延情報を入力し(ステップ1)、入力された遅延時間に基づいて遅延時間を決定し(ステップ2)、決定された遅延時間に応じて、演算に適用する遅延時間を変化させて乗乗剰余演算を行う(ステップ3)。

【0008】また、上記のステップ1において、乱数を生成するために必要な初期値を生成し、初期値に基づいて乱数を生成し、生成した乱数から遅延時間を生成する。また、本発明は、乱数生成に用いる初期値を生成する際に、複数の初期値を生成し、生成された複数の初期値から乱数を生成する。

【0009】また、本発明は、乱数生成に用いる初期値を生成する際に、乗乗剰余演算中の初期値を更新する。また、本発明は、初期値を更新する際に、乗乗剰余演算中の途中結果の一部または全部を用いて、以降の乱数の初期値を更新する。

【0010】図2は、本発明の原理構成図である。本発明は、乗乗剰余演算を実行する乗乗剰余演算装置であって、乗乗剰余の演算時間を変化させるための情報を入力する変化情報入力手段10と、変化情報入力手段10により入力された変化情報に基づいて遅延時間を決定する遅延時間決定手段20と、遅延時間決定手段20により決定された遅延時間に基づいて乗乗剰余演算を行う乗乗剰余演算手段30とを有する。

【0011】また、上記の変化情報入力手段10は、乱数を生成するために必要な初期値を入力する乱数初期値入力手段11と、乱数初期値入力手段により入力された初期値に基づいて乱数を生成し、変化情報として遅延時間決定手段に入力する乱数生成手段12とを含み、遅延時間決定手段20は、乱数生成手段12により入力され

た乱数に基づいて遅延時間を決定する手段を含む。

【0012】また、上記の乱数初期値入力手段11は、乱数を生成するために必要な初期値を外部から入力する第1の乱数初期値入力手段を含む。また、上記の乱数初期値入力手段11は、乱数を生成するための必要な初期値を装置内部で生成する第2の乱数初期値入力手段を含む。

【0013】また、上記の乱数初期値入力手段11は、第1の乱数初期値入力手段により入力された初期値と、第2の乱数初期値入力手段により入力された初期値とを合成した値を乱数生成手段への入力とする初期値合成手段を含む。また、上記の遅延時間決定手段20は、乗乗剰余演算手段30の実行中に遅延時間を更新する遅延時間更新手段を含む。

【0014】また、上記の変化情報入力手段10は、乗乗剰余演算手段30の実行中の演算結果を用いて、以降の乱数生成手段12の初期値を更新する演算結果循環型初期値更新手段を含む。図3に、送信者端末が署名を演算し、その結果を受信者に向けて送信する場合の基本的な例を示す。

【0015】送信者101は、通信をモニタして解析し、秘密鍵を推測しようとする。最も解析しやすい(危険性の高い)順は、送信者端末の付近102、通信網103、受信者端末の付近104である。この最大の理由は、送信者の送信者端末102に近いほど、通信等に関わる処理の割合が少ないからである。また、モニタしやすいところは、公衆網(通信網)の部分である。

【0016】最も解析しやすい場合の例を考える。即ち、送信者端末102に乗乗剰余演算専用のプロセッサが搭載されていて、そのプロセッサの演算時間、公開鍵等の公開情報、演算結果を得ることができると仮定する。それらの結果を複数蓄積し、演算に用いた秘密鍵を推測することが目的となる。

【0017】上記の環境が最も解析し易い最大の原因是、同一入力であれば、同じ演算時間になり、専用プロセッサであるため他の処理に殆ど影響がないためである。そこで、本発明は、専用プロセッサを用いた場合、同一入力でも毎回異なる演算時間になるように、不確定の遅延時間を持つ回路をプロセッサ内に設けるか、外部からランダムな遅延時間を与えることにより、タイミングアタックに対する防御として大変有効である。

【0018】

【発明の実施の形態】図4は、本発明の乗乗剰余演算装置の構成を示す。同図に示す乗乗剰余演算装置は、遅延時間調整部202、遅延時間決定部203を有する乗乗剰余演算部201、乱数発生部204、初期値合成部205、初期値発生部207、演算結果フィードバック部208から構成され、初期値合成部205には、外部初期値入力部206が乗乗剰余演算装置の外部から接続される。

【0019】通常の乗乗剰余演算部の多くのハードウェアの回路には、伝搬遅延によるクリティカルパスの遅延時間調整する回路があり、通常の設計では、遅延時間調整回路を必要最小限にする。本発明では、この遅延時間調整回路の遅延時間を乗乗演算基に変化させることにより、同一の値を用いた乗乗演算であっても遅延時間が異なるように設計する。

【0020】乗乗剰余演算部201は、遅延時間調整部202と遅延時間決定部203を有することにより、必要最小限の遅延時間を遅延時間決定部203で決定した遅延時間を遅延時間調整部202に与えて、演算時間を変化させる。乱数発生部204は、遅延時間決定部203で決定される遅延時間がランダムとなるように乱数を発生させる。乱数発生部204で発生した乱数を遅延時間決定部203に与える。その乱数発生部204で発生する乱数は、初期値の入力によって決定される。その初期値の生成方法として以下の3つに大別できる。

【0021】① 乗乗剰余演算装置の外部に接続される外部初期値入力部206から入力された値により生成する。

② 乗乗剰余演算装置内部の初期値発生部207で発生した初期値により生成する。

【0022】③ 乗乗剰余演算装置内部の演算結果フィードバック部208で以前の演算結果に基づいて生成する。初期値合成部205は、初期値の生成方法として、外部初期値入力部206からの初期値、初期発生部207で生成された初期値、演算結果フィードバック部208からフィードバックされた演算結果を初期値とする。いずれか単独で用いてもよいが、それぞれの初期値を合成する初期値合成部205を利用して、上記の①、②、③の方法を組み合わせることにより、より質のよい乱数を生成することが可能となる。

【0023】

【実施例】以下に、本発明の実施例を図面と共に説明する。図5は、本発明の一実施例の乗乗剰余演算方法の一連の動作を示すフローチャートである。

【0024】図4の構成に基づいて図5のフローチャートを説明する。ステップ101) まず、初期値合成部205は、外部初期値入力部206からの外部初期値の入力があるかを判定する。外部入力がある場合には、ステップ102に移行する。外部初期値の入力がない場合には、ステップ103に移行する。

【0025】ステップ102) 外部入力がある場合には、外部初期値入力部206から乱数発生のための初期値が入力され、初期値合成部205は当該初期値を保持する。ステップ103) 初期値合成部205は、初期値発生部207からの内部初期値の生成があるかを判定し、ある場合には、ステップ104に移行し、内部初期値の生成がない場合には、ステップ105に移行する。

【0026】ステップ104) 初期値発生部207か

らの内部初期値が生成された場合には、初期値合成部205は、当該内部初期値を保持する。ステップ105)

乗乗剰余演算部201における演算結果を初期値としてフィードバックするかどうかを判定し、演算結果を初期値としてフィードバックする場合は、ステップ106に移行し、フィードバックしない場合には、ステップ107に移行する。

【0027】ステップ106) 演算結果をフィードバックする場合には、フィードバック部208において、演算結果を初期値としてフィードバックして、初期値合成部205にフィードバックする。ステップ107) 初期値合成部205は、ステップ102、ステップ104、ステップ106のいずれか、または、全てにおいて入力された初期値を合成する。合成の方法は、本発明では特に限定しないが、次の乱数生成の初期値(シード)として使用可能な値である必要がある。初期値合成部205は、合成した初期値を乱数発生部204に転送する。

【0028】ステップ108) 乱数発生部204は、初期値合成部205から渡された初期値を用いて乱数を生成し、乗乗剰余演算部201の遅延時間決定部203に転送する。ステップ109) 乗乗剰余演算部201の遅延時間決定部203は、取得した乱数から遅延時間を決定し、遅延時間調整部202では、決定された遅延時間に回路設計から決まる最低限必要な遅延時間を加え、これを最終的な遅延時間とする。

【0029】なお、上記の一連の処理において、初期値合成部205において、外部初期値入力部206、装置内部の初期値発生部207または、演算結果フィードバック部208から入力される値を初期値としているが、初期値合成部205では、予め1つの初期値入力のみを用いるようにしてよいし、入力された全ての初期値を用いるようにしてもよい。これらの選択を所定の周期で変更する等の方法も考えられる。また、外部初期値入力部206や、初期値発生部207または、演算結果フィードバック部208をランダムに起動させることも可能である。

【0030】上記の実施例に示したように、秘密鍵演算である乗乗剰余演算において、全て同じパラメタを使用しても、遅延時間を乗乗剰余演算基に変化させることにより、仮に、正確に演算時間を計測されたとしても秘密鍵を導出することは困難である。

【0031】なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内において、乗乗剰余演算基に遅延時間を変化させる方法であればよい。

【0032】

【発明の効果】上述のように、本発明の乗乗剰余演算方法及び装置によれば、乗乗剰余演算を利用した公開鍵暗号の攻撃方法として、危険性が高かったタイミングアタックに対する防御に有効である。特に、他の処理の影響

を殆ど受けることがない、専用プロセスを利用した場合に効果的である。

【図面の簡単な説明】

【図1】本発明の原理を説明するための図である。

【図2】本発明の原理構成図である。

【図3】タイミングアタックが起こり得る場合の環境を示した概念図である。

【図4】本発明の審査割余演算装置の内部構成図である。

【図5】本発明の一実施例の審査割余演算方法の一連の動作を示すフローチャートである。

【符号の説明】

10 10 变化情報入力手段

11 11 亂数初期値入力手段

12 12 亂数生成手段

* 20 20 遅延時間決定手段

30 30 審査割余演算手段

101 101 受信者

102 102 送信者端末

103 103 通信御

104 104 受信者端末

201 201 審査割余演算部

202 202 遅延時間調整部

203 203 遅延時間決定部

204 204 亂数発生部

205 205 初期値生成部

206 206 外部初期値入力部

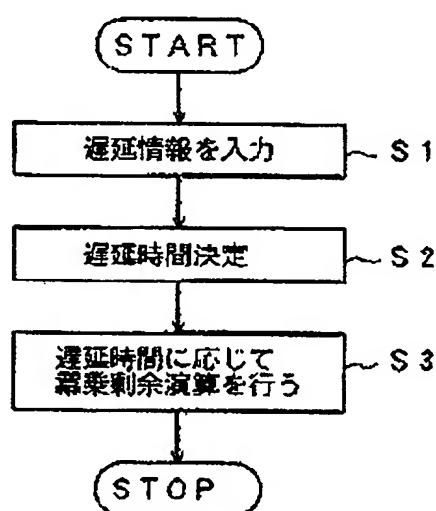
207 207 初期値発生部

208 208 演算結果フィードバック部

*

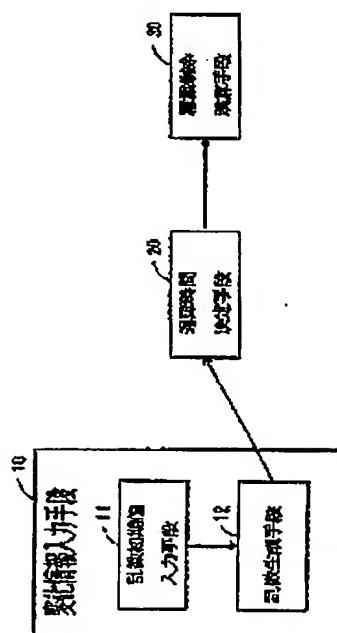
【図1】

本発明の原理を説明するための図



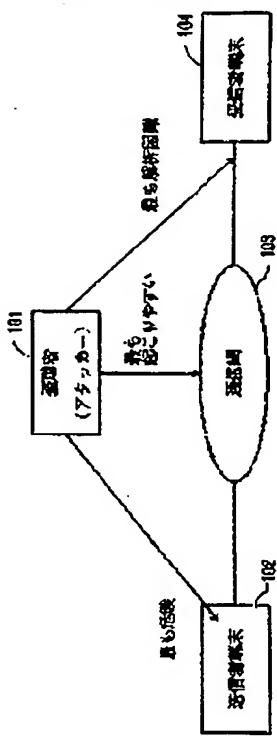
【図2】

本発明の原理構成図



【図3】

タイミングアタックが起こりうる場合の構造を示した概要図



【図4】

本発明の構成による攻撃装置の内構成図

